(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－285284
（P2001－285284A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
H04L	9/32		G06F	12/14	320A	5B017
G06F	12/14	320		13/00	540S	5J104
	13/00	540	H04L	9/00	673B	5K030
H04L	12/28			11/00	310Z	5K033
	12/22			11/26		

審査請求　未請求　請求項の数10　ＯＬ　（全 6 頁）

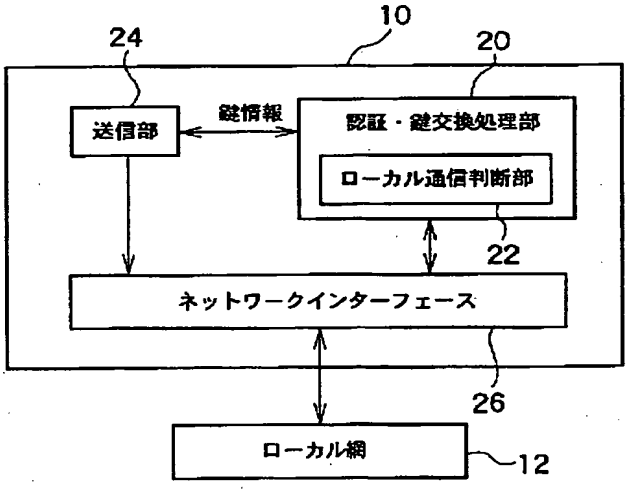
(21)出願番号　特願2000－94851(P2000－94851)
(22)出願日　平成12年３月30日(2000.3.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　送信装置およびその送信方法

(57)【要約】
【課題】　ローカル網上に存在する受信装置のみと認証・鍵交換を実行することで、著作権保護を考慮して著作物を受信装置に送信できる送信装置、およびその送信方法を提供する。
【解決手段】　ローカル網１２に接続された送信装置１０である。この送信装置１０は、受信装置１８ａに、暗号化された、映画、音楽等の著作物を含むデータを送信する送信部２４と、受信装置１８ａがローカル網１２に接続されているか否かを判断するローカル通信判断部２２と、ローカル網１２に接続されていると判断された場合のみ、受信装置１８ａとの間で、認証・鍵交換を実行する認証・鍵交換部２０と、から構成される。



【特許請求の範囲】

【請求項１】　特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であって、

該受信装置に暗号化データを送信する送信部と、

前記受信装置が前記ローカル網に接続されているか否かを判断する判断部と、

前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する認証・鍵交換部とを有することを特徴とする送信装置。

【請求項２】　前記認証・鍵交換部は、前記受信装置が前記ローカル網に接続されていないと判断した場合には、前記受信装置からの認証・鍵交換要求を拒絶する、ことを特徴とする請求項１に記載の送信装置。

【請求項３】　前記判断部は、前記送信装置および受信装置の両方が、前記ローカル網に割り当てられた同一のアドレス上に存在するか否かを検知する手段、を備える、ことを特徴とする請求項１に記載の送信装置。

【請求項４】　前記検知手段は、前記受信装置から送られたパケットのサブネットIDが前記送信装置のサブネットIDと一致するか否かを照合する手段、を備える、ことを特徴とする請求項３に記載の送信装置。

【請求項５】　前記判断部は、前記受信装置から送られるパケットのスコープフィールドを用いて、前記送信装置および受信装置の両方が、同一のローカルスコープ内に存在するか否かを検知する手段を備える、ことを特徴とする請求項１に記載の送信装置。

【請求項６】　前記受信装置から送られるパケットは、前記受信装置からの、前記送信装置に対するデータ送信要求または認証・鍵交換要求を構成するパケットである、ことを特徴とする請求項４または５に記載の送信装置。

【請求項７】　特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、

該受信装置からのデータ送信要求を受け取る工程と、

該データ送信要求に基づき、前記受信装置に暗号化データを送信する工程と、

前記受信装置からの認証要求を受け取る工程と、

前記受信装置が前記ローカル網に接続されているか否かを判断する工程と、

前記受信装置が前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する工程とを含むことを特徴とする送信方法。

【請求項８】　前記判断工程は、前記受信装置が、前記ローカル網に割り当てられたアドレス上に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。

【請求項９】　前記判断工程は、前記受信装置が、送信装置と同一のローカルスコープ内に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。

【請求項１０】　前記判断工程の後に、前記受信装置が前記ローカル網に接続されていないと判断された場合のみ、前記受信装置に認証不許可通知を送信する工程を、さらに含む、ことを特徴とする請求項７に記載の送信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権保護を実現する機能を備えた送信装置およびその送信方法に関する。

【０００２】

【従来の技術】近年の、デジタル化・ネットワーク化の進展に伴って、デジタル情報家電と呼ばれる商品が増加して来ている。デジタル情報家電は、デジタル放送の開始に伴い、普及が期待される商品群である。このデジタル情報家電には、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等、デジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。

【０００３】このようなデジタル情報家電を利用する際に、考慮すべき事柄の一つとして、著作物の著作権による保護、が挙げられる。デジタルデータは、コピー時の品質劣化がない等の利点が強調される反面、不正コピーが容易である等の欠点を持っているためである。たとえばデジタルAV機器どうしを接続するデジタルネットワークであるIEEE1394には、著作権侵害の防止のため、認証・鍵交換機構や、データ暗号化の機能が備えられる。

【０００４】ここで、著作権保護が必要なAVデータを、送信装置から受信装置に転送する場合を考える。この転送において、注意すべき点は、個人あるいは家族の楽しむ範囲内で、著作権保護の必要なAVデータのやり取りを行なうことが、著作権保護の前提である点である。そして、他人との間でのAVデータのやり取りは、視聴料や著作権料等の支払いが伴わない限り、行われるべきではないという点である。

【０００５】

【発明が解決しようとする課題】近い将来、デジタルネットワークの種類は、無線や、パソコンネットワーク等、いろいろな種類に増加するものと考えられるが、これらの多くについては、未だ著作権保護が考慮されていないのが現状である。

【０００６】また、ネットワークはローカルなものからグローバルなものまで幅広くあり、上記で説明したように、著作権保護の観点からは、明確に区別することが必要がある。

【０００７】本発明は、このような課題を解決し、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交

換を実行できる送信装置、およびその送信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明は、特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であり、受信装置に暗号化データを送信する送信部と、受信装置がローカル網に接続されているか否かを判断する判断部と、ローカル網に接続されていると判断された受信装置のみとの間で、認証・鍵交換を実行する認証・鍵交換部と、から構成される送信装置であることを第１の特徴とする。ここで、「ローカル網」とは、個人の範囲内、あるいは家族間でのデータのやりとりが行なわれる網であり、たとえばIEEE1394等のホームネットワークである。

【０００９】本発明の第１の特徴では、このローカル網内に閉じた通信のみを、個人あるいは家族間で楽しむための通信とみなすことで、著作権保護を行なうべきデータのやりとりを許容する。そして、このローカル網で閉じない通信は、個人あるいは家族間で楽しむための通信とみなすことができないため、著作権保護を行なうべきデータのやりとりを許容しない。このため、データ再生を要求する受信装置がローカル網上に存在するか否かをあらかじめ判断し、その判断結果に基づいて、受信装置と認証・鍵交換を実行することで、著作権保護を考慮したデータのやりとりが可能となる。すなわち、ローカル網に接続された受信装置のみが、認証・鍵交換を実行し、それにより、暗号化されたデータを復号できるようになる。

【００１０】本発明の第２の特徴は、上記の第１の特徴で述べた送信装置が実現する送信方法に係り、特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、その受信装置からのデータ送信要求を受け取る工程と、そのデータ送信要求に基づき、受信装置に暗号化データを送信する工程と、受信装置からの認証要求を受け取る工程と、受信装置がローカル網に接続されているか否かを判断する工程と、受信装置がローカル網に接続されていると判断された場合のみ、受信装置との間で、認証・鍵交換を実行する工程と、を少なくとも含む送信方法であることである。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【００１２】図１は、本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。図１に示すように、本発明の実施の形態に係る送信装置１０は、イーサネット（登録商標）等のローカル網１２に接続される。そして、ローカル網１２にルータ１４が接続され、ルータ１４によって、ローカル網１０とインターネット１６とが接続される。ローカル網１２には受信装置１８ａが接続され、インターネット１６には受信装置１８ｂが接続され、受信装置１８ａおよび１８ｂの両方が、送信装置１０から送信されるAVデータを受信しようとすることになる。AVデータとしてはたとえば、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等が挙げられる。ここでは、説明の簡単化を図るため、AVデータの一部に著作物が含まれる、あるいはAVデータ自体が著作物であるとする。

【００１３】ここで、送信装置１０から受信装置１８ａおよび１８ｂに、著作権保護の必要なAVデータを転送する場合を考える。この場合、注意すべき点は、従来の技術の説明でも述べたように、個人、あるいは拡大解釈して家族の楽しむ範囲内で、AVデータのやりとりを行なうことが著作権保護の前提であり、他人との間のAVデータのやりとりは、視聴料や著作権料の支払いが伴わない限り、行なわれるべきではないということである。たとえば他人との間でのデータのやりとりとしては、インターネットや電話網等の公衆網を介したオープンな通信が挙げられ、個人の範囲内、あるいは家庭間のデータのやりとりの典型例として、IEEE1394等のホームネットワークに閉じた通信が挙げられる。

【００１４】そこで、著作権保護を行なうため、図１のネットワーク・システムにおけるAVデータの転送に関し、次の２つの規則を用いる。

【００１５】（Ａ）ローカル網１２に閉じた通信は、著作権保護を行なうべきAVデータのやりとりを許容する。

【００１６】（Ｂ）ローカル網１２で閉じない通信は、著作権保護を行なうべきAVデータのやりとりを許容しない。

【００１７】ここで、上記（Ａ）の規則は、ローカル網１２で閉じた通信は、個人あるいは家庭間で楽しむための通信と見なすことができるからであり、上記（Ｂ）の規則は、ローカル網１２で閉じない通信は、個人あるいは家庭間で楽しむための通信と、通常、見なすことができないからである。

【００１８】図２は、本発明の実施の形態に係る送信装置の構成を示すブロック図である。図２に示すように、この実施の形態に係る送信装置１０は、受信装置１８（１８ａ，１８ｂ）との間での認証・鍵交換処理を実行する認証・鍵交換処理部２０と、認証・鍵交換処理を要求する受信装置１８との通信が、上記の（Ａ）および（Ｂ）の規則のいずれに該当するかを判断するローカル通信判断部２２と、暗号化されたAVデータを受信装置１８に送信する送信部２４と、ローカル網１２とのインターフェースとなるネットワークインターフェース２６と、から構成される。図２では、ローカル通信判断部２

2は、認証・鍵交換処理部２０内に配置されているが、もちろん、認証・鍵交換処理部２０外に配置されてももちろん構わない。

【００１９】次に、図３ないし図５を参照して、本発明の実施の形態に係る送信装置の動作について説明する。図３は、本発明の実施の形態に係る送信装置１０と、ローカル網１２に接続された受信装置１８ａと、の間の処理シーケンスチャートであり、図４は、本発明の実施の形態に係る送信装置１０と、インターネット１６に接続された受信装置１８ｂと、の間の処理シーケンスチャートであり、図５は、本発明の実施の形態に係る送信装置１０の送信方法の処理手順を示すフローチャートである。

【００２０】（イ）送信装置１０と受信装置１８ａとの間の通信

（１）図３のステップＳ１０１において、受信装置１８ａが、ローカル網１２を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００２１】（２）図３のステップＳ１０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２を介して、受信装置１８ａに送信する（図５のステップＳ３０２）。

【００２２】（３）図３のステップＳ１０３において、暗号化されたAVデータを受信した受信装置１８ａは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００２３】（４）図３のステップＳ１０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１８ａがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。ローカル網１２上に存在すると判断できる基準として、たとえば次の２つが挙げられる。

【００２４】（C）認証・鍵交換要求パケットのソースアドレス、すなわち受信装置１８ａのアドレス、のサブネットIDが、送信装置１０自身のサブネットIDと一致すること。

【００２５】（D）IPv6パケットのスコープフィールドがローカルスコープを示していること。

【００２６】なお、この判断は、受信装置１８ａからの再生要求のパケットに基づいて、実行しても、もちろん構わない。また、これら再生要求のパケットおよび認証・鍵交換要求のパケットは、その転送中に、改ざん等がなされてしまうと、正確な判断を行なうことができなくなる。このため、各パケットのソースアドレスおよびスコープフィールドそれぞれの値に、改ざん検出のための署名等を施すべきである。

【００２７】（５）受信装置１８ａはローカル網１２上に存在するので（図５のステップＳ３０４ＹＥＳ）、図３のステップＳ１０５において、送信装置１０は、受信装置１８ａとの間で、認証・鍵交換を実行する（図５のステップＳ３０６）。この認証・鍵交換によって、受信装置１８ａは、暗号化ＡＶデータの復号のために必要な復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、復号鍵は暗号化鍵K1と同一である。

【００２８】（６）図３のステップＳ１０６において、復号鍵K1を入手した受信装置１８ａは、先に受信したAVデータを復号する。

【００２９】（ロ）送信装置１０と受信装置１８ｂとの間の通信

（１）図４のステップＳ２０１において、受信装置１８ｂが、インターネット１６、ルータ１４およびローカル網１２、を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。上記（イ）の場合と同様、AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００３０】（２）図４のステップＳ２０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２、ルータ１４およびインタネット１６を介して、受信装置１８ｂに送信する（図５のステップＳ３０２）。

【００３１】（３）図４のステップＳ２０３において、暗号化されたAVデータを受信した受信装置１８ｂは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００３２】（４）図４のステップＳ２０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１０ｂがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。

【００３３】（５）受信装置１８ｂはローカル網１２上に存在しないので（図５のステップＳ３０４ＮＯ）、図４のステップＳ２０５において、送信装置１０は、受信装置１８ｂに対して、認証不許可を通知する（図５のステップＳ３０５）。この認証不許可によって、受信装置１８ｂは、先に受信したAVデータを復号するために必要な復号鍵を入手することができない。このため、ローカル網１２上に存在しない受信装置１８ｂが、不正にAVデータを入手することを、未然に防ぐことが可能となる。

【００３４】このように、本発明の実施の形態によれば、ローカル網上に存在する受信装置のみに対して、著作権保護の必要なAVデータを送信することが可能となる。このため、近年のデジタル化・ネットワーク化に伴って増加する一方である、ネットワーク上で送信される

著作物を適切に保護することが可能となり、その重要性はきわめて高いものである。

【００３５】

【発明の効果】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信装置を実現できる。

【００３６】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信方法を実現できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。

【図２】本発明の実施の形態に係る送信装置の具体的な構成を示すブロック図である。

【図３】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

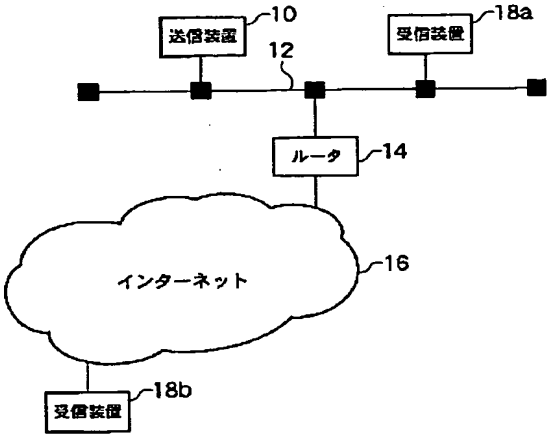
【図４】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

【図５】本発明の実施の形態に係る送信装置の送信方法の処理手順を示すフローチャートである。

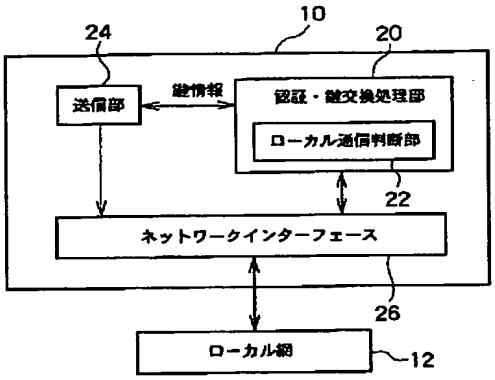
【符号の説明】

１０　送信装置
１２　ローカル網
１４　ルータ
１６　インターネット
１８　受信装置
２０　認証・鍵交換処理部
２２　ローカル通信判断部
２４　送信部
２６　ネットワークインターフェース

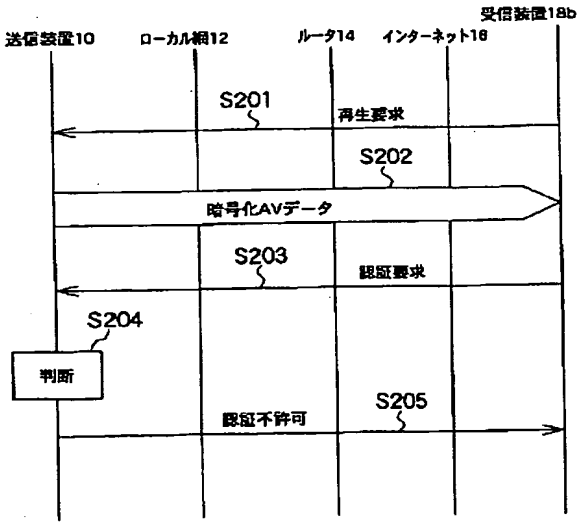
【図１】



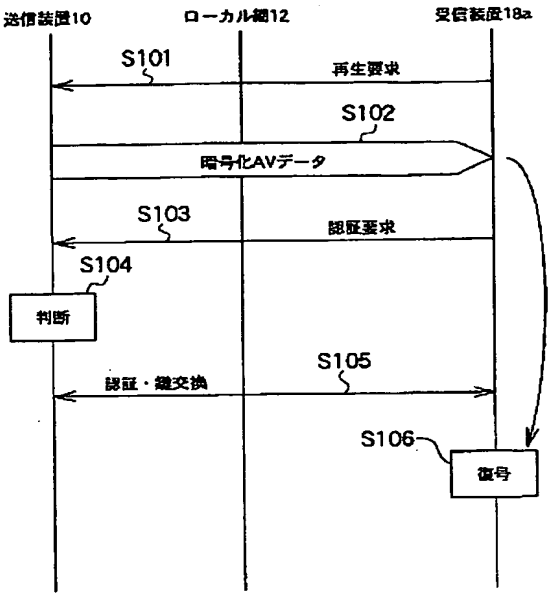
【図２】



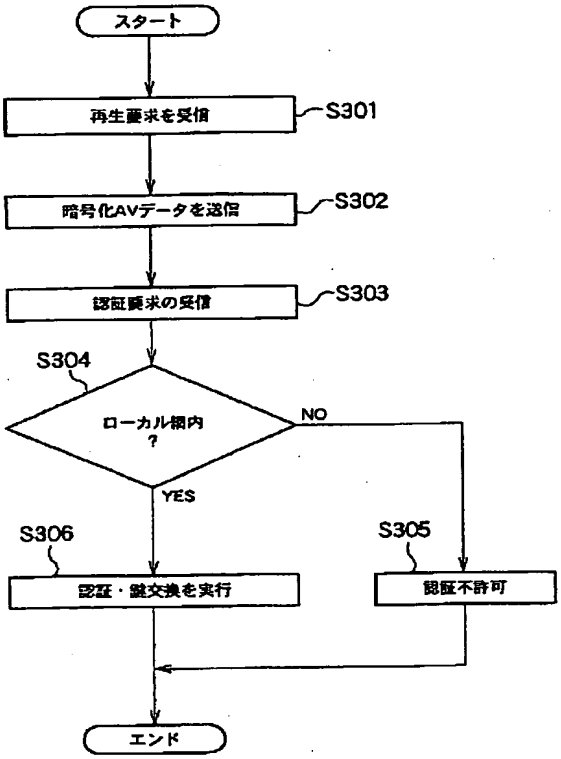
【図４】



【図３】



【図５】



フロントページの続き

Ｆターム(参考) 5B017 AA03 BA05 BA07 CA16
5J104 AA07 AA12 AA16 EA04 EA15
KA02 PA07
5K030 GA15 HA08 HB21 HC14 JL09
JT04 LD20
5K033 AA08 BA01 BA15 CB01 DA01
DA13